le réseau

➔ Qu'est-ce qu'un réseau ?

un réseau informatique est un ensemble de dispositifs (ordinateurs, périphériques, reliés entre eux par des moyens matériels et logiciels pour echanger des donnees et partager des ressources il utilise un protocole de communication pour permettre aux dispositifs de se reconnaître et de communiquer

➔ À quoi sert un réseau informatique ?

1. Partager des données.
2. Partager des ressources physiques, comme des imprimantes et des scanners.
3. Partager des applications et des logiciels sans les installer.
4. Stocker et sauvegarder des données de manière centralisée.
5. Rechercher des informations sur internet.
6. Communiquer à distance.
7. Partager la puissance de calcul et la capacité de stockage.

➔ Quel matériel avons-nous besoin pour construire un réseau ?

- Les ordinateurs : Plusieurs ordinateurs fonctionnels disposant des cartes réseau Ethernet et/ou wifi.
- Le routeur : Il permet de relier les réseaux et ainsi de faire circuler (router) des données d'un réseau à un autre de façon optimale.

Le switch ou commutateur : C'est un équipement qui relie divers éléments (par câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet. Un

commutateur sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Il segmente donc le réseau.

- Le Modem : Le modem (pour modulateur-démodulateur), est un périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'une ligne téléphonique. Il permet par exemple de se connecter à Internet.
- Le Firewall ou pare-feu : Son rôle est de sécuriser votre réseau. Le firewall est constitué de différents matériels et logiciels qui vont se charger de séparer votre réseau privé d'un réseau public externe, ou d'autres réseaux non sécurisés.
- Le serveur : Dans un réseau informatique, un serveur est à la fois un ensemble de logiciels et l'ordinateur hébergeant dont le rôle est de répondre de manière automatique à des demandes de services envoyées par des clients via le réseau.
- La passerelle : Une entreprise peut comporter plusieurs réseaux locaux utilisant les moyens de communication (protocoles) différents. Dans ce cas, il est indispensable de procéder à une conversion de protocoles pour relier ces réseaux locaux entre eux.

Quels cables avez-vous choisis pour relier les deux ordinateurs ?

Un câble Ethernet droit est un type de câble qui est utilisé pour connecter des types de dispositifs différents dans un réseau. Par exemple, un câble droit pour connecter un ordinateur à un switch ou un routeur

Cependant, lorsque vous connectez deux dispositifs similaires, comme deux ordinateurs, ont utiliseriez normalement un câble "croisé". Un câble croisé a les fils à chaque extrémité disposés dans des ordres différents, ce qui permet aux deux dispositifs de communiquer directement entre eux sans avoir besoin d'un dispositif de réseau intermédiaire.

Cela dit, de nombreux dispositifs modernes sont capables de détecter automatiquement le type de câble et d'ajuster leur communication en conséquence. Cette fonctionnalité, appelée Auto-MDIX, peut permettre à deux ordinateurs de se connecter avec un câble droit.

Une adresse IP, ou adresse de protocole Internet, est une série de chiffres qui identifie de manière unique un dispositif connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Les adresses IP sont essentielles pour le routage des données sur Internet. Elles servent à identifier l'emplacement d'un dispositif sur un réseau et à lui permettre de communiquer avec d'autres dispositifs.

Il existe deux versions principales d'adresses IP : IPv4 (Internet Protocol version 4) et IPv6 (Internet Protocol version 6). Les adresses IPv4 sont composées de quatre groupes de chiffres séparés par des points, par exemple, 192.168.1.1. Les adresses IPv6 sont plus longues et composées de huit groupes de caractères alphanumériques, séparés par des deux-points, par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Les adresses IP sont utilisées pour diriger le trafic sur Internet et à l'intérieur des réseaux locaux. Elles sont essentielles pour permettre aux ordinateurs, aux serveurs, aux routeurs et à d'autres dispositifs de se connecter et de communiquer efficacement au sein d'un réseau et sur Internet.

➔ À quoi sert un IP ?

Un IP, ou "adresse IP" (Internet Protocol address en anglais), est un identifiant numérique unique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet (IP). Les adresses IP servent à plusieurs fins importantes, notamment :

Identification des appareils : Les adresses IP sont utilisées pour identifier de manière unique chaque appareil connecté à un réseau, que ce soit un ordinateur, un smartphone, un serveur, un routeur, une imprimante

Communication sur Internet : Lorsque vous accédez à des sites Web, envoyez des e-mails, partagez des fichiers ou effectuez d'autres activités en ligne, votre adresse IP est utilisée pour permettre la communication entre votre appareil et les serveurs distants.

Sécurité réseau : Les adresses IP sont utilisées dans le cadre de la sécurité réseau pour contrôler l'accès aux ressources, définir des règles de pare-feu, surveiller le trafic et détecter les activités suspectes.

Attribution dynamique d'adresses : Les fournisseurs de services Internet (FSI) attribuent souvent des adresses IP dynamiques à leurs clients, ce qui signifie que l'adresse IP peut changer à chaque connexion. Cela permet d'optimiser l'utilisation des adresses IP disponibles.

Configuration de réseaux locaux : Sur un réseau local (LAN), les adresses IP sont utilisées pour identifier chaque appareil, permettant ainsi la communication et le partage de ressources au sein du réseau

➔ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control address) est un identifiant unique attribué à une carte réseau ou à une interface réseau d'un appareil informatique. Contrairement à une adresse IP (Internet Protocol address) qui est utilisée pour identifier un appareil sur un réseau IP, une adresse MAC est utilisée pour identifier un appareil au niveau de la couche de liaison de données d'un réseau, généralement au sein d'un réseau local LAN

Chaque carte réseau (carte Ethernet, Wi-Fi, etc.) fabriquée par un constructeur a une adresse MAC unique qui lui est assignée en usine. Cela signifie que deux appareils ne devraient pas avoir la même adresse MAC.

Ne traverse pas les routeurs : Contrairement aux adresses IP, les adresses MAC ne sont généralement pas transmises au-delà du réseau local. Cela signifie que l'adresse MAC d'un appareil n'est pas visible sur Internet ou sur d'autres réseaux distants.

Configuration matérielle : Les adresses MAC sont liées au matériel spécifique de la carte réseau de l'appareil. Elles ne sont pas généralement configurables par l'utilisateur et ne changent pas, sauf en cas de remplacement de la carte réseau.

➔ Qu'est-ce qu'une IP publique et privée ?

Adresse IP publique :

Une adresse IP publique est utilisée pour identifier un appareil ou un réseau sur Internet.Elle est unique et routable sur Internet, ce qui signifie qu'elle peut être utilisée pour communiquer directement avec des appareils et des serveurs situés à travers le monde.

Une adresse IP privée est utilisée pour identifier un appareil au sein d'un réseau local (Local Area Network, LAN) privé, tel qu'un réseau domestique ou un réseau d'entreprise.

Les adresses IP privées ne sont pas routables sur Internet. Cela signifie qu'elles ne sont pas directement accessibles depuis l'extérieur du réseau local.

Les adresses IP privées sont essentielles pour permettre aux appareils d'un réseau local de communiquer entre eux, tandis que l'adresse IP publique est utilisée pour la communication avec des appareils situés en dehors du réseau local, notamment sur Internet. L'utilisation d'adresses IP privées contribue également à renforcer la sécurité en masquant les appareils du réseau local derrière une seule adresse IP publique, ce qui rend plus difficile pour des entités extérieures d'accéder directement à ces appareils.

➔ Quelle est l'adresse de ce réseau ?

➔ Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?

La ligne de commande pour voir les adresse ip sont : ipconfig /all

pc pierre :

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0050.0FB3.EC76
   Link-local IPv6 Address.........: FE80::250:FFF:FEB3:EC76
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-09-68-29-8E-00-50-0F-B3-EC-76
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 0000.0CBD.53E7
   Link-local IPv6 Address.........: ::
--More--
```

Pc Alicia :

```
ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.639A.60C3
   Link-local IPv6 Address.........: FE80::201:63FF:FE9A:60C3
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-20-B0-19-79-00-01-63-9A-60-C3
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 00E0.F724.B414
   Link-local IPv6 Address.........: ::
--More--
```

➔ Quelle est la commande permettant de Ping entre des PC ?

la commande est : ping suivi de l'adresse ip de la personne

pc alicia connecte au pc de pierre :

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pc pierre connecte au pc d'alicia :

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Éteignez le PC de Pierre. Utilisez le terminal du PC d'Alicia et PING le PC le Pierre. Faites une capture d'écran du terminal d'Alicia.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

➔ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

NON

➔ Expliquez pourquoi.

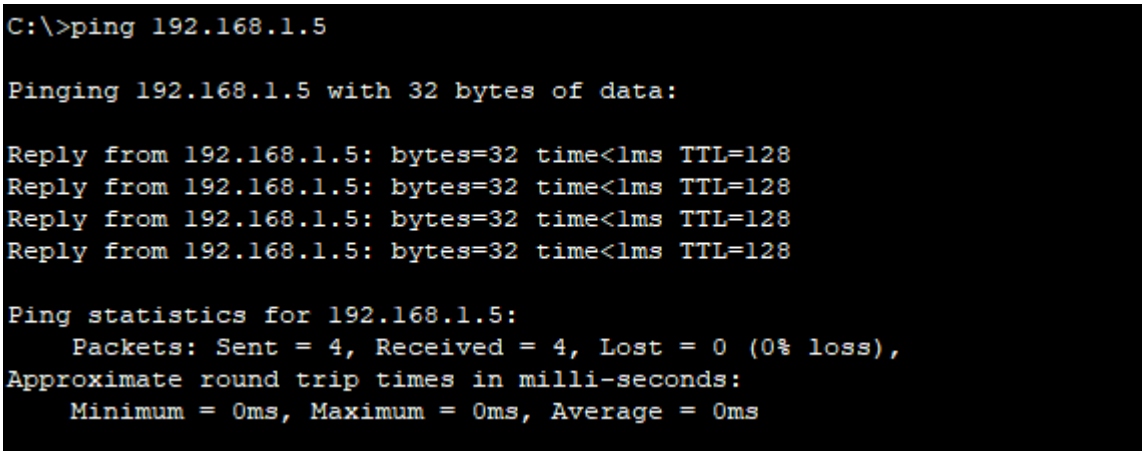
Si ont éteint le PC de Pierre et ensuite, à partir du PC d'Alicia, et que j'essaie de faire un ping vers le PC de Pierre, le PC de Pierre ne recevra pas les paquets envoyés par Alicia. La raison en est que lorsque j'éteins un ordinateur, il n'est plus connecté au réseau. Par conséquent, il ne peut pas recevoir de paquets réseau.

La commande ping envoie des paquets ICMP Echo Request à l'adresse IP spécifiée et attend une réponse. Si l'ordinateur est éteint, il ne peut pas répondre aux paquets Echo Request avec des paquets Echo Reply. Par conséquent, la commande ping affichera probablement une erreur ou un délai d'attente.

Agrandissez votre sous réseau avec cinq ordinateurs, et configurez vos ordinateurs sur

le même réseau. Vérifiez qu'ils soient tous bien connectés en affectant un PING en

utilisant le terminal prompt.



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
```

➔ Quelle est la différence entre un hub et un switch ?

Différence entre un hub et un switch : Les hubs et les switchs sont des équipements informatiques utilisés pour relier des ordinateurs sur un réseau. La principale différence entre les deux est que le hub transmet tous les paquets à l'ensemble des machines , tandis que le switch se contente de transmettre les paquets à leur véritable destinataire uniquement

➔ Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

avantages et inconvénients d'un hub : Un hub est un périphérique réseau qui relie plusieurs ordinateurs entre eux et relaie immédiatement les données qu'il reçoit. Lorsqu'un hub reçoit des données, il

transfère l'intégralité de celles-ci à tous les appareils connectés sur le mode du semi-duplex. Cependant, tous les appareils reçoivent donc le paquet de données en question, même si celui-ci ne leur est pas initialement destiné. Cela génère beaucoup de charge sur le réseau et peut conduire à des temps de réponse plus longs.

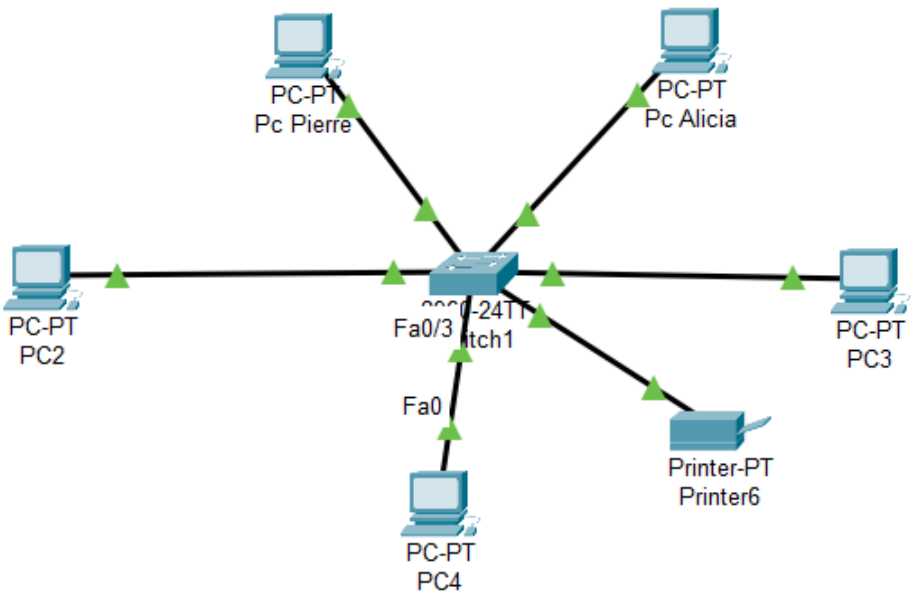
➔ Quels sont les avantages et inconvénients d'un switch ?

Avantages et inconvénients d'un switch : Un switch réseau est un équipement qui permet d'interconnecter plusieurs ordinateurs sur un même réseau. Il a l'avantage d'opérer un filtrage des paquets reçus, et de les transférer uniquement au destinataire prévu. Mais le trafic de diffusion peut être problématique.

➔ Comment un switch gère-t-il le trafic réseau ?

Un switch est un périphérique matériel responsable du pontage du réseau, transférant les données vers la destination souhaitée avec précision en fonction de l'adresse MAC. Il est utilisé pour diriger le trafic dans la bonne direction. Si un appareil essaie de récupérer des données depuis une autre source, le switch vérifiera s'il connaît cette destination. Dans la négative, il enverra les données à un autre appareil comme un routeur pour laisser ce dernier gérer.

Réalisez un schéma de votre réseau en utilisant le logiciel de votre choix



identifiez au moins trois avantages importants d'avoir un schéma

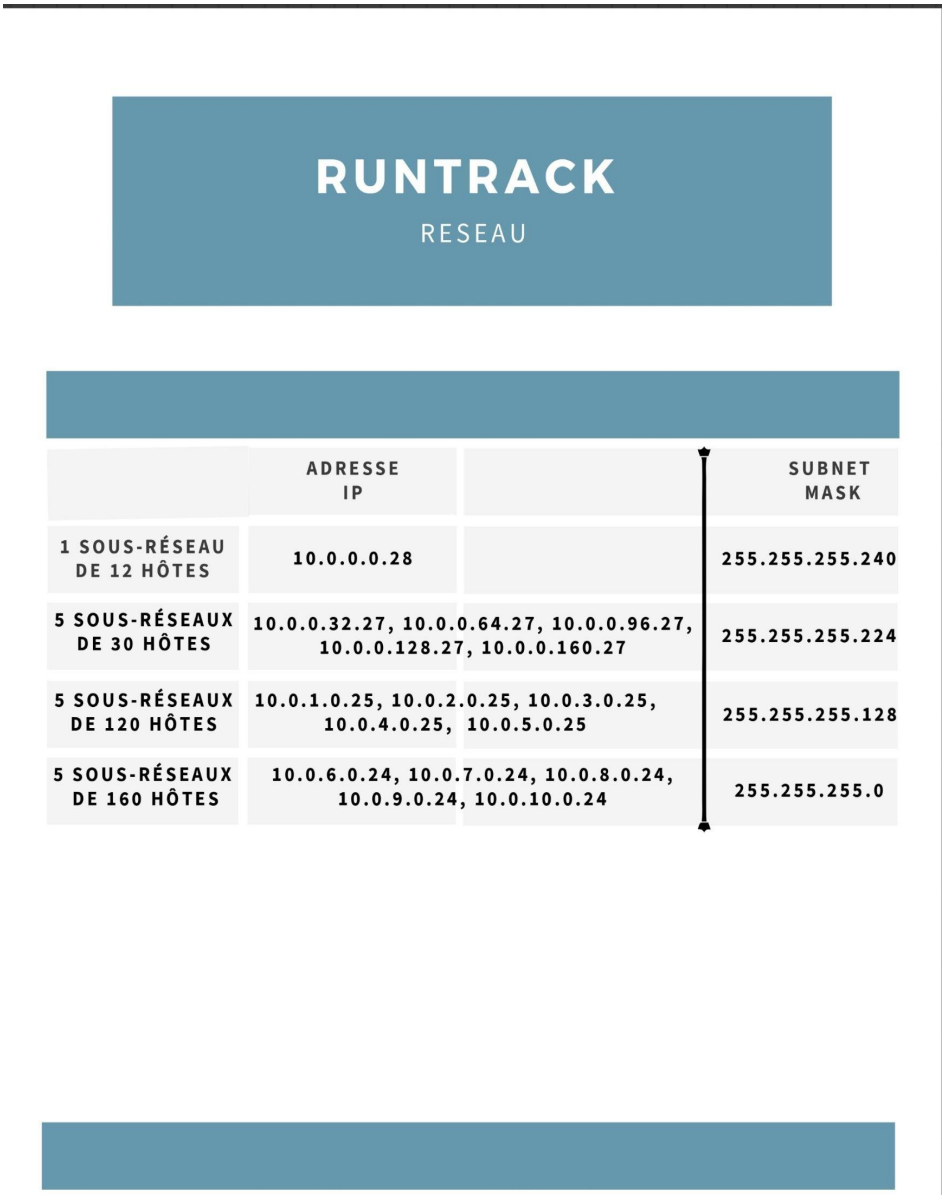
1. **Compréhension claire** : Un schéma de réseau donne une vue d'ensemble claire de la façon dont le réseau est configuré. Il aide à comprendre comment les différents composants sont connectés entre eux.
2.
3. **Dépannage** : En cas de problème de réseau, le schéma peut aider à identifier rapidement où se situe le problème.

4. **Planification et expansion** : Si on prévoit d'ajouter de nouveaux appareils ou de modifier la configuration de votre réseau, un schéma peut aider à planifier ces changements de manière efficace.

➔ Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

La différence clé entre une adresse IP statique et une adresse IP attribuée par DHCP est que l'adresse IP statique est fixe et ne change pas, tandis que l'adresse IP attribuée par DHCP peut changer de temps en temps.

Creation de sous réseau



➔ Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

Le choix d'une adresse de classe A comme 10.0.0.0 offre un grand nombre d'adresses IP possibles, C'est utile pour les grands réseaux avec de nombreux sous-réseaux et hôtes. l'adresse 10.0.0.0 permet d'avoir jusqu'à 16 777 214 hôtes par réseau.

ET comme c'est une adresse privée, elle peut être utilisée librement sur un réseau interne sans risque de conflit avec des adresses IP utilisées sur internet.

➔ Quelle est la différence entre les différents types d'adresses ?

Il existe différentes classes d'adresses IP (A, B, C, D et E) qui déterminent comment l'adresse est divisée entre la partie réseau et la partie hôte de l'adresse. Les classes A, B et C sont utilisées pour les adresses publiques, tandis que les classes D et E sont réservées à des fins particulières.

Créez un tableau dans lequel se trouvent les sept couches du modèle OSI, avec chaque couche une description des rôles.

Couche	Nom	Description	Matériels/Protocoles
7 Application	Fournit des services réseau aux applications logicielles.	HTML, FTP, SSL/TLS	
6 Présentation	Traduit les données entre le format du réseau et le format que l'application peut comprendre.	SSL/TLS	
5 Session	Établit, gère et termine les connexions entre les applications locales et distantes.	PPTP	
4 Transport	Fournit un transfert de données fiable et sans erreur entre les systèmes.	TCP, UDP	
3 Réseau	Détermine la meilleure façon de router les paquets de données vers leur destination.	IPv4, IPv6, routeur	
2 Liaison de données	Définit le format des données sur le réseau. Une connexion de réseau (NIC) et un commutateur fonctionnent à cette couche.	Ethernet, MAC, Wi-Fi, fibre optique, câble RJ45	
1 Physique	Transmet des bits bruts sur le support de transmission. Cette couche fournit des moyens mécaniques, électriques, fonctionnels et procéduraux pour activer, maintenir et désactiver les liaisons physiques entre les systèmes.	Fibre optique, Wi-Fi, câble RJ45	

➔ Quelle est l’architecture de ce réseau ?

➔ Indiquer quelle est l’adresse IP du réseau ?

➔ Déterminer le nombre de machines que l’on peut brancher sur ce réseau ?

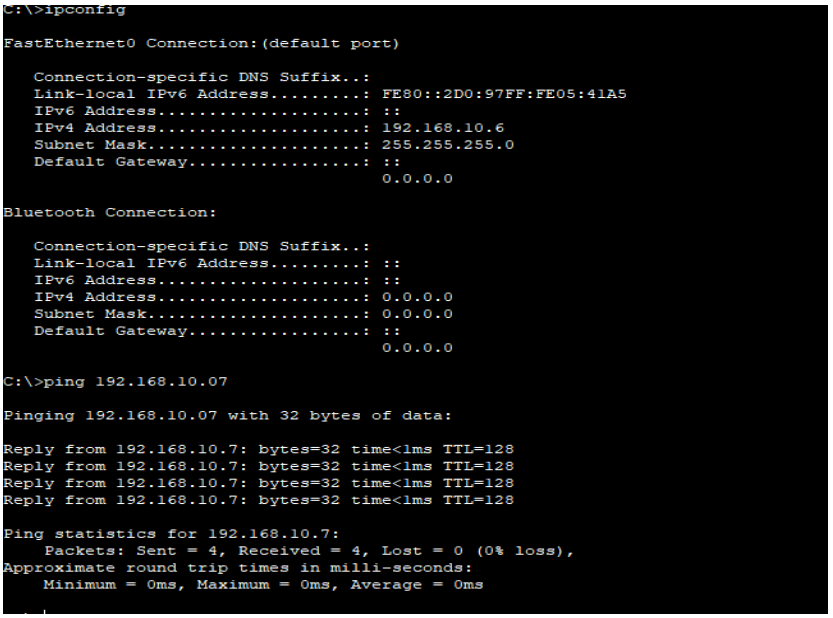
➔ Quelle est l’adresse de diffusion de ce réseau ?

Ce réseau est configuré en étoile, ce qui signifie que chaque appareil, comme un PC ou un serveur, est connecté à un point central appelé commutateur.

L'adresse IP du réseau peut être identifiée en effectuant une sorte d'opération logique spéciale avec n'importe quelle adresse IP du réseau et un numéro appelé "masque de sous-réseau." Dans ce cas, l'adresse IP du réseau est 192.168.10.0.

Le nombre de machines que vous pouvez connecter à ce réseau est déterminé par le masque de sous-réseau, qui est ici 255.255.255.0. En gros, cela signifie que les trois premiers groupes de chiffres de l'adresse IP sont réservés pour désigner le réseau lui-même, tandis que le dernier groupe de chiffres est utilisé pour les appareils connectés. Cela signifie qu'il y a de la place pour un maximum de 254 appareils (en excluant deux adresses spéciales).

Une de ces adresses spéciales est l'adresse de diffusion, qui est la manière d'envoyer un message à tous les appareils du réseau en une seule fois. Dans ce cas, cette adresse serait 192.168.10.255.



Convertissez les adresses IP suivantes en binaires :

● 145.32.59.24

● 200.42.129.16

● 14.82.19.54

- 145.32.59.24 se convertit en **10010001.00100000.00111011.00011000**
- 200.42.129.16 se convertit en **11001000.00101010.10000001.00010000**
- 14.82.19.54 se convertit en **00001110.01010010.00010011.00110110**

➔ Qu'est-ce que le routage ?

Le routage est un processus qui se produit dans un réseau pour acheminer les données d'un expéditeur à un ou plusieurs destinataires. Le routage est exécuté par des dispositifs de la couche réseau, appelés routeurs. Les routeurs utilisent des tables de routage pour déterminer le chemin le plus efficace ou le plus optimal pour livrer les paquets.

➔ Qu'est-ce qu'un gateway ?

Un gateway ou une passerelle, est un dispositif matériel de réseau ou un nœud de réseau conçu pour connecter deux réseaux différents, permettant aux utilisateurs de communiquer à travers plusieurs réseaux. Les passerelles les plus courantes sont les ordinateurs et routeurs qui relient une entreprise à un réseau.

➔ Qu'est-ce qu'un VPN ?

Un VPN est un service qui aide à préserver la confidentialité en ligne en chiffrant la connexion entre l'es appareil et Internet. Cette connexion sécurisée fournit un tunnel privé pour les données et communications lorsque qu'on utilise des réseaux publics.

➔ Qu'est-ce qu'un DNS ?

Le DNS est le système qui permet de trouver l'adresse IP d'un site web à partir de son nom de domaine. Le DNS repose sur une base de données répartie et hiérarchisée, contenant des enregistrements appelés RR. Ces enregistrements ont une durée de vie limitée, appelée TTL, qui indique aux serveurs intermédiaires quand ils doivent vérifier les informations